## REMARKS

Claims 1-28 are pending and under consideration. Claim 1 is amended herein. Claim 29 is cancelled herein, without prejudice or disclaimer. Support for the amendment to claim 1 may be found in the specification at page 4, lines 21 and 22, and in claims 3 and 18 as filed originally. This amendment is believed to place the application in condition for allowance, and entry therefore is respectfully requested. In the alternative, entry of this amendment is requested as placing the application in better condition for appeal by, at least, reducing the number of issues outstanding. Further reconsideration is requested based on the foregoing amendment and the following remarks.

**Response to Arguments:**

The Applicants appreciate the consideration given to their arguments. The Applicants, however, are disappointed that their arguments were not found to be persuasive. The final Office Action responds to the argument that neither Hasebe, Ginter, Chen, nor Shear teach, disclose, or suggest, "storing the encrypted predetermined information in an area outside said predetermined secure area," in section 5 at page 2 by asserting:

> However, Hasebe discloses storing permissions information on a recording medium (portable card) (Fig. 2). Chen teaches that it is useful in reducing costs, to occasionally backup the data on an IC card to a storage medium (p.1, ¶1-3) and therefore it is submitted that it would have been obvious to modify Hasebe to backup the permission information on the portable card. Hence, Hasebe, as modified above, teaches storing encrypted predetermined information in an are outside said predetermined area (in a backup storage medium).

Neither Hasebe nor Chen, however, show storing encrypted predetermined information anywhere outside of where it was output from the encryptor. Chen has no encrypted data at all. Hasebe simply dumps the encrypted permission information 13 out of the encrypting unit 23 onto storage medium 14. Permission information 13 is never stored anywhere else before it is decrypted in decrypting unit 32. Thus, if storage medium 14 is used to meet the recitation "an area outside said predetermined secure area," then storage medium 14 is not available to meet the recitation "a predetermined secure area of a recording medium."

Consequently, since permission information 13 is decrypted before it is stored again, permission information 13 cannot meet the recitation "storing the encrypted predetermined information in an area outside said predetermined secure area." Chen cannot either, since no encrypted data is mentioned in Chen, let alone storage thereof, at all. Thus, the combination

lacks the elements required to meet the claim, regardless of whether it is obvious to combine them or not.

The final Office Action apparently notes the lack of the claimed "storing the encrypted predetermined information in an area outside said predetermined secure area," in any of the cited references, and asserts in section 8 at page 3 that:

> While little patentable weight is given to the phrase "secure area", as it is not a standard term and the claim does not define it further, Hasebe does not explicitly disclose that the area in which the permissions information is stored is a "secure area". Shear teaches that it is useful to store certain data in a hidden area, which is inaccessible to certain readers (p. 15, ¶218).

To the contrary, in one embodiment, the recited secure area is defined in the specification at page 4, lines 21 and 22 as an area that cannot be controlled by an external source. Even if the location on disk 100 not normally accessible of Shear were ascribed to Hasebe, there is still no showing of "storing the encrypted predetermined information in an area outside said predetermined secure area." Still, in the interest of compact patent prosecution, and not for any reason of patentability, claim 1 has been amended in consideration with the Examiner's implied suggestion to define "secure area" further. The secure area was already defined as not subject to control by external instructions in claim 18, so that claim has not been amended. The Applicants appreciate the Examiner's suggestion.

Finally, in section 9 at page 3, the final Office Action responds to the argument that persons of ordinary skill in the art would have been deterred from modifying Hasebe in the manner proposed because Hasebe "warns against illegal copying" by asserting that:

> However, Hasebe's invention solves this problem by encrypting the data, which does not affect the combination proposed.

To the contrary, the modification proposed in the final Office Action would negate the encryption scheme of Hasebe by storing the permissions information on a freely copyable IC card. Thus, anyone who wanted permission to access the encrypted data could simply acquire a copy of the IC card.

Further reconsideration is thus requested.

**Claim Rejections - 35 U.S.C. § 103:**

Claims 1-7, 9, 11, 13, 18, 19, 21, 23, and 25-28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,392,351 to Hasebe et al., (hereinafter "Hasebe"), in view of U.S. Patent No. 5,892,900 to Ginter et al. (hereinafter "Ginter"), UK Patent Application

GB 2 284 689 to Chen (hereinafter "Chen"), and U.S. Patent Application No. 2001/0042043 to Shear et al. (hereinafter "Shear"). The rejection is traversed. Reconsideration is earnestly solicited.

The third clause of claim 1 recites:

> Storing the encrypted predetermined information in an area outside said predetermined secure area.

Neither Hasebe, Ginter, Chen, nor Shear teach, disclose, or suggest "storing the encrypted predetermined information in an area outside said predetermined secure area," as recited in claim 1. Thus even if Hasebe, Ginter, Chen, and Shear were combined, as proposed in the final Office Action, the claimed invention would not result.

The final Office Action, in fact, acknowledges Hasebe shows no storage of encrypted predetermined information in an area outside a predetermined secure area. The final Office Action seeks to compensate for this deficiency of Hasebe by combining Hasebe with Chen, saying that backing up an IC card as described in Chen at page 1, paragraphs [0001]-[0003] is equivalent to storage of encrypted predetermined information in an area outside a predetermined secure area. This is submitted to be incorrect.

Backing up an IC card, rather, is not the same as "storing the encrypted predetermined information in an area outside said predetermined secure area," as recited in claim 1. In the first place, the IC card of Chen really has no encrypted predetermined information to store. Rather, as described page 1, lines 6, 7, and 8 of Chen,

> Most portable data providing devices, such as electronic dictionaries, employ an IC card to expand its database or to upgrade the functions of the same.

The IC card of Chen is thus employed to expand databases or to upgrade the functions of portable data providing devices, such as electronic dictionaries, not "storing the encrypted predetermined information in an area outside said predetermined secure area," as recited in claim 1. No mention of encryption appears in Chen at all.

Ginter, for its part, shows no "storing the encrypted predetermined information in an area outside said predetermined secure area," as recited in claim 1, either. In Ginter, rather, as described at column 173, lines 30-33,

> Instead, back up routine 1250 encrypts each secure database 610 item with a newly generated back up key(s) (block 1256) and writes the encrypted item to back up store 668 (block 1258). This process continues until all items within secure database 610 have been read, decrypted, encrypted with a newly

> generated back up key(s), and written to the back up store (as tested for by decision block 1260).

Thus, Ginter doesn't even bother trying to figure out what the encryption key held by SPU 500 might have been, let alone "storing the encrypted predetermined information in an area outside said predetermined secure area," as recited in claim 1. Ginter, rather, just creates new encryption keys whenever it needs them.

Finally, Shear shows no "storing the encrypted predetermined information in an area outside said predetermined secure area," as recited in claim 1, either. In Shear, rather, as described at paragraph [0218],

> In the example shown in FIG. 3, disk 100 stores one or more decryption keys for decrypting key block 208 on the medium itself in the form of a hidden key(s) 210. Hidden key(s) 210 may be stored, for example, in a location on disk 100 not normally accessible.

Thus, hidden key(s) 210 of Shear are stored in an inaccessible, i.e. secure location on disk 100, rather than "storing the encrypted predetermined information in an area outside said predetermined secure area," as recited in claim 1. Or, in the alternative, as described in Shear at paragraph [0219],

> Alternatively, and/or in addition, keys required to decrypt encrypted key block 208 could be provided by disk drive 80. In this example, disk drive 80 might include a small decryption component such as, for example, an integrated circuit decryption engine including a small secure internal key store memory 212 having keys stored therein. Disk drive 80 could use this key store 212 in order to decrypt encrypted key block 208 without exposing either keys 212 or decrypted key block 208--and then use the decrypted key from key block 208 to decrypt protected content 200, 202.

This is to be contrasted with claim 1, which recites "storing the encrypted predetermined information in an area outside said predetermined secure area." Thus, even if Hasebe, Ginter, Chen, and Shear were combined, as suggested by the final Office Action, the claimed invention would not result.

Furthermore, persons of ordinary skill in the art who read Hasebe for all it contained at the time the invention was made would have been deterred from modifying Hasebe in the manner proposed in the final Office Action and thus, even if the combination included the elements of the claimed invention, it would not have been obvious. Hasebe, in particular, warns against illegal copying at column 1, lines 18-24, where he notes,

> However, it is relatively easy for a third party to illegally copy electronic data. As a result of illegal copying, a vendor of electronic data suffers significant damage in

> that he cannot derive legitimate benefits. As a result of this damage, the cost of electronic data, i.e., the software and electronically published data rises so that users also suffer due to increased prices.

Copying software illegally is technically equivalent to copying software for back-up purposes. Copying is copying. The computer will never know the difference. The only difference between making an illegal copy of software and backing up software is the intention of the copier. Furthermore, the economic effect of which Hasebe warns are the same in each case, the vendor of electronic data derives no benefits, legitimate or otherwise, from the backed-up software, either. The vendor would certainly prefer that a customer bought back-up copies from the vendor, rather than making them themselves. Therefore, persons of ordinary skill in the art would have not been motivated to combine the references as suggested by the final Office Action, since Hasebe warns against (illegal) copying. Claim 1 is submitted to be allowable. Withdrawal of the rejection of claim 1 is earnestly solicited.

Claims 2-7, 9, 11, 13, and 27 depend from claim 1 and add additional distinguishing elements. Claims 2-7, 9, 11, 13, and 27 are thus also submitted to be allowable. Withdrawal of the rejection of claims 2-7, 9, 11, 13, and 27 is earnestly solicited.

Claims 18, 19, 21, 23, 25, 26, and 28:

> The third clause of claim 18 recites:
>
> Storing the encrypted predetermined information in an area outside said secure area.

Neither Hasebe, Ginter, Chen, nor Shear teach, disclose, or suggest "storing the encrypted predetermined information in an area outside said secure area," as discussed above with respect to claim 1. Claim 18 is thus submitted to be allowable as well, for at least those reasons discussed above with respect to claim 1. Withdrawal of the rejection of claim 18 is earnestly solicited.

Claims 19, 21, 23, 25, 26, and 28 depend from claim 18 and add additional distinguishing elements. Claims 19, 21, 23, 25, 26, and 28 are thus also submitted to be allowable. Withdrawal of the rejection of claims 19, 21, 23, 25, 26, and 28 is earnestly solicited.

Claims 8, 10, 12, 14-17, 20, 22, and 24:

Claims 8, 10, 12, 14-17, 20, 22, and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hasebe, Ginter, Chen, and Shear, and further in view of U.S. Patent No.

5,191,611 to Lang. (hereinafter "Lang"). The rejection is traversed. Reconsideration is earnestly solicited.

Claims 8, 10, 12, and 14-17 depend from claim 1 and add additional distinguishing elements. Neither Hasebe, Ginter, Chen, nor Shear teach, disclose, or suggest "storing the encrypted predetermined information in an area outside said secure area," as discussed above with respect to claim 1. Lang shows no "storing the encrypted predetermined information in an area outside said predetermined secure area," either, and thus cannot compensate for the deficiencies of Hasebe, Ginter, Chen, and Shear with respect to claims 8, 10, 12, and 14-17. In Lang, rather, as described at column 2, lines 42-47,

> Additionally, a storage accessing device (used interchangeably herein with the following terms--personal accessing device (PAD) and smart card) provided with an encrypted or non-encrypted personal security key as well as personal identification code is included to allow an individual access to the storage medium or media.

Thus, a storage accessing device in Lang is provided with an encrypted or non-encrypted personal security key. No mention "storing the encrypted predetermined information in an area outside said predetermined secure area," as recited in claim 1, appears in Lang at all.

Or else, as described at column 4, lines 2-8,

> Alternatively, the decryption algorithm can be stored on the smart card and the decryption of information would take place in the smart card and this information is then transferred to the computer for viewing and processing.

This is to be contrasted with claim 1, which recites, "storing the encrypted predetermined information in an area outside said predetermined secure area." Claims 8, 10, 12, and 14-17 are thus also submitted to be allowable. Withdrawal of the rejection of claims 8, 10, 12, and 14-17 is earnestly solicited.

Claims 20, 22, and 24:

Claims 20, 22, and 24 depend from claim 18 and add additional distinguishing elements. Neither Hasebe, Ginter, Chen, nor Shear teach, disclose, or suggest "storing the encrypted predetermined information in an area outside said secure area," as discussed above with respect to claim 1. Lang shows no storage of encrypted predetermined information in an area outside a predetermined secure area either, and thus cannot compensate for the deficiencies of Hasebe, Ginter, Chen, and Shear with respect to claims 20, 22, and 24. Claims 20, 22, and 24 are thus also submitted to be allowable. Withdrawal of the rejection of claims 20, 22, and 24 is earnestly solicited.

**Conclusion:**

Accordingly, in view of the reasons given above, it is submitted that all of claims 1-28 are allowable over the cited references. Allowance of all claims 1-28 and of this entire application is therefore respectfully requested.

If there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 08/1/06

By: _____
Thomas E. McKiernan
Registration No. 37,889

1201 New York Ave, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501